

ON PERIOD POLYNOMIALS OF DEGREE 2^m FOR FINITE FIELDS

IOULIA N. BAOULINA

ABSTRACT. We obtain explicit factorizations of reduced period polynomials of degree 2^m , $m \geq 4$, for finite fields of characteristic $p \equiv 3$ or $5 \pmod{8}$. This extends the results of G. Myerson, who considered the cases $m = 1$ and $m = 2$, and S. Gurak, who studied the case $m = 3$.

Keywords: Period polynomial; cyclotomic period; f -nomial period; reduced period polynomial; Gauss sum; Jacobi sum; factorization.

2010 Mathematics Subject Classification: 11L05, 11T22, 11T24

1. INTRODUCTION

Let \mathbb{F}_q be a finite field of characteristic p with $q = p^s$ elements, $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$, and let γ be a fixed generator of the cyclic group \mathbb{F}_q^* . By $\text{Tr} : \mathbb{F}_q \rightarrow \mathbb{F}_p$ we denote the trace mapping, that is, $\text{Tr}(x) = x + x^p + x^{p^2} + \cdots + x^{p^{s-1}}$ for $x \in \mathbb{F}_q$. Let e and f be positive integers such that $q = ef + 1$. Denote by \mathcal{H} the subgroup of e -th powers in \mathbb{F}_q^* . For any positive integer n , write $\zeta_n = \exp(2\pi i/n)$.

The cyclotomic (or f -nomial) periods of order e for \mathbb{F}_q with respect to γ are defined by

$$\eta_k = \sum_{x \in \gamma^k \mathcal{H}} \zeta_p^{\text{Tr}(x)} = \sum_{h=0}^{f-1} \zeta_p^{\text{Tr}(\gamma^{eh+k})}, \quad k = 0, 1, \dots, e-1.$$

The period polynomial of degree e for \mathbb{F}_q is the polynomial

$$P_e(X) = \prod_{k=0}^{e-1} (X - \eta_k).$$

The reduced cyclotomic (or reduced f -nomial) periods of order e for \mathbb{F}_q with respect to γ are defined by

$$\eta_k^* = \sum_{x \in \mathbb{F}_q} \zeta_p^{\text{Tr}(\gamma^k x^e)} = 1 + e\eta_k, \quad k = 0, 1, \dots, e-1,$$

and the reduced period polynomial of degree e for \mathbb{F}_q is

$$P_e^*(X) = \prod_{k=0}^{e-1} (X - \eta_k^*).$$

The polynomials $P_e(X)$ and $P_e^*(X)$ have integer coefficients and are independent of the choice of generator γ . They are irreducible over the rationals when $s = 1$, but not necessarily irreducible when $s > 1$. More precisely, $P_e(X)$ and $P_e^*(X)$ split over the

rational factors into $\delta = \gcd(e, (q-1)/(p-1))$ factors of degree e/δ (not necessarily distinct), and each of these factors is irreducible or a power of an irreducible polynomial. Furthermore, the polynomials $P_e(X)$ and $P_e^*(X)$ are irreducible over the rationals if and only if $\gcd(e, (q-1)/(p-1)) = 1$. For proofs of these facts, see [10].

In the case $s = 1$, the period polynomials were determined explicitly by Gauss for $e \in \{2, 3, 4\}$ and by many others for certain small values of e . In the general case, Myerson [10] derived the explicit formulas for $P_e(X)$ and $P_e^*(X)$ when $e \in \{2, 3, 4\}$, and also found their factorizations into irreducible polynomials over the rationals. Gurak [7] obtained similar results for $e \in \{6, 8, 12, 24\}$; see also [6] for the case $s = 2$, $e \in \{6, 8, 12\}$. Note that if -1 is a power of p modulo e , then the period polynomials can also be easily obtained. Indeed, if $e > 2$ and $e \mid (p^\ell + 1)$, with ℓ chosen minimal, then $2\ell \mid s$, and [10, Proposition 20] yields

$$P_e^*(X) = (X + (-1)^{s/2\ell}(e-1)q^{1/2})(X - (-1)^{s/2\ell}q^{1/2})^{e-1}.$$

Baumert and Mykkeltveit [3] found the values of cyclotomic periods in the case when $e > 3$ is a prime, $e \equiv 3 \pmod{4}$ and p generates the quadratic residues modulo e ; see also [10, Proposition 21].

It is seen immediately from the definitions that $P_e(X) = e^{-e}P_e^*(eX + 1)$, and so it suffices to factorize only $P_e^*(X)$.

The aim of this paper is to obtain the explicit factorizations of the reduced period polynomials of degree 2^m with $m \geq 4$ in the case that $p \equiv 3$ or $5 \pmod{8}$. Notice that in this case $\text{ord}_2(q-1) = \text{ord}_2(p^s-1) = \text{ord}_2 s + 2$. Hence, for $p \equiv 3 \pmod{8}$,

$$\gcd(2^m, (q-1)/(p-1)) = \begin{cases} 2^m & \text{if } 2^{m-1} \mid s, \\ 2^{m-1} & \text{if } 2^{m-2} \parallel s. \end{cases}$$

Appealing to [10, Theorem 4], we conclude that in the case when $2^{m-1} \mid s$, $P_{2^m}^*(X)$ splits over the rationals into linear factors. If $2^{m-2} \parallel s$, then $P_{2^m}^*(X)$ splits into irreducible polynomials of degrees at most 2. Similarly, for $p \equiv 5 \pmod{8}$,

$$\gcd(2^m, (q-1)/(p-1)) = \begin{cases} 2^m & \text{if } 2^m \mid s, \\ 2^{m-1} & \text{if } 2^{m-1} \parallel s, \\ 2^{m-2} & \text{if } 2^{m-2} \parallel s. \end{cases}$$

Using [10, Theorem 4] again, we see that $P_{2^m}^*(X)$ splits over the rationals into linear factors if $2^m \mid s$, splits into linear and quadratic irreducible factors if $2^{m-1} \parallel s$, and splits into linear, quadratic and biquadratic irreducible factors if $2^{m-2} \parallel s$. Our main results are Theorems 3.2 and 4.2, which give the explicit factorizations of $P_{2^m}^*(X)$ in the cases $p \equiv 3 \pmod{8}$ and $p \equiv 5 \pmod{8}$, respectively. All the evaluations in Sections 3 and 4 are effected in terms of parameters occurring in quadratic partitions of some powers of p .

2. PRELIMINARY LEMMAS

In the remainder of the paper, we assume that p is an odd prime. Let ψ be a nontrivial character on \mathbb{F}_q . We extend ψ to all of \mathbb{F}_q by setting $\psi(0) = 0$. The Gauss sum $G(\psi)$ over

\mathbb{F}_q is defined by

$$G(\psi) = \sum_{x \in \mathbb{F}_q} \psi(x) \zeta_p^{\text{Tr}(x)}.$$

Gauss sums occur in the Fourier expansion of a reduced cyclotomic period.

Lemma 2.1. *Let ψ be a character of order $e > 1$ on \mathbb{F}_q such that $\psi(\gamma) = \zeta_e$. Then for $k = 0, 1, \dots, e-1$,*

$$\eta_k^* = \sum_{j=1}^{e-1} G(\psi^j) \zeta_e^{-jk}.$$

Proof. It follows from [4, Theorem 1.1.3 and Equation (1.1.4)]. \square

In the next three lemmas, we record some properties of Gauss sums which will be used throughout this paper. By ρ we denote the quadratic character on \mathbb{F}_q ($\rho(x) = +1, -1, 0$ according as x is a square, a non-square or zero in \mathbb{F}_q).

Lemma 2.2. *Let ψ be a nontrivial character on \mathbb{F}_q with $\psi \neq \rho$. Then*

- (a) $G(\psi)G(\bar{\psi}) = \psi(-1)q$;
- (b) $G(\psi) = G(\psi^p)$;
- (c) $G(\psi)G(\psi\rho) = \bar{\psi}(4)G(\psi^2)G(\rho)$.

Proof. See [4, Theorems 1.1.4(a, d) and 11.3.5] or [9, Theorem 5.12(iv, v) and Corollary 5.29]. \square

Lemma 2.3. *We have*

$$G(\rho) = \begin{cases} (-1)^{s-1} q^{1/2} & \text{if } p \equiv 1 \pmod{4}, \\ (-1)^{s-1} i^s q^{1/2} & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

Proof. See [4, Theorem 11.5.4] or [9, Theorem 5.15]. \square

Lemma 2.4. *Let $p \equiv 3 \pmod{8}$, $2 \mid s$ and ψ be a biquadratic character on \mathbb{F}_q . Then $G(\psi) = -q^{1/2}$.*

Proof. It is a special case of [4, Theorem 11.6.3]. \square

Let ψ be a nontrivial character on \mathbb{F}_q . The Jacobi sum $J(\psi)$ over \mathbb{F}_q is defined by

$$J(\psi) = \sum_{x \in \mathbb{F}_q} \psi(x) \psi(1-x).$$

The following lemma gives a relationship between Gauss sums and Jacobi sums.

Lemma 2.5. *Let ψ be a nontrivial character on \mathbb{F}_q with $\psi \neq \rho$. Then*

$$G(\psi)^2 = G(\psi^2)J(\psi).$$

Proof. See [4, Theorem 2.1.3(a)] or [9, Theorem 5.21]. \square

Let ψ be a character on \mathbb{F}_q . The lift ψ' of the character ψ from \mathbb{F}_q to the extension field \mathbb{F}_{q^r} is given by

$$\psi'(x) = \psi(N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(x)), \quad x \in \mathbb{F}_{q^r},$$

where $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(x) = x \cdot x^q \cdot x^{q^2} \cdots x^{q^{r-1}} = x^{(q^r-1)/(q-1)}$ is the norm of x from \mathbb{F}_{q^r} to \mathbb{F}_q .

Lemma 2.6. *Let ψ be a character on \mathbb{F}_q and let ψ' denote the lift of ψ from \mathbb{F}_q to \mathbb{F}_{q^r} . Then*

- (a) ψ' is a character on \mathbb{F}_{q^r} ;
- (b) a character λ on \mathbb{F}_{q^r} equals the lift ψ' of some character ψ on \mathbb{F}_q if and only if the order of λ divides $q - 1$;
- (c) ψ' and ψ have the same order.

Proof. See [4, Theorem 11.4.4(a, c, e)]. □

The following lemma, which is due to Davenport and Hasse, connects a Gauss sum and its lift.

Lemma 2.7. *Let ψ be a nontrivial character on \mathbb{F}_q and let ψ' denote the lift of ψ from \mathbb{F}_q to \mathbb{F}_{q^r} . Then*

$$G(\psi') = (-1)^{r-1} G(\psi)^r.$$

Proof. See [4, Theorem 11.5.2] or [9, Theorem 5.14]. □

Now we turn to the case $p \equiv 3$ or $5 \pmod{8}$. We recall a few facts which were established in our earlier paper [2] in more general settings.

Lemma 2.8. *Let $p \equiv 3$ or $5 \pmod{8}$ and ψ be a character of order 2^r on \mathbb{F}_q , where*

$$r \geq \begin{cases} 4 & \text{if } p \equiv 3 \pmod{8}, \\ 3 & \text{if } p \equiv 5 \pmod{8}. \end{cases}$$

Then $G(\psi) = G(\psi\rho)$.

Proof. See [2, Lemma 2.13]. □

Lemma 2.9. *Let $p \equiv 3$ or $5 \pmod{8}$, $r \geq 3$, and ψ be a character of order 2^r on \mathbb{F}_q . Then*

$$\psi(4) = \begin{cases} 1 & \text{if } p \equiv 3 \pmod{8}, \\ (-1)^{s/2^{r-2}} & \text{if } p \equiv 5 \pmod{8}. \end{cases}$$

Proof. See [2, Lemma 2.16]. □

Lemma 2.10. *Let $p \equiv 3$ or $5 \pmod{8}$, $n \geq 1$ and $r \geq 3$ be integers, $r \geq n$. Then*

$$\sum_{v=0}^{2^{r-2}-1} \zeta_{2^n}^{p^v} = \begin{cases} -2^{r-2} & \text{if } n = 1, \\ 2^{r-2}i & \text{if } n = 2 \text{ and } p \equiv 5 \pmod{8}, \\ 2^{r-3}i\sqrt{2} & \text{if } n = 3 \text{ and } p \equiv 3 \pmod{8}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. It is an immediate consequence of [2, Lemma 2.2]. □

The next lemma relates Gauss sums over \mathbb{F}_q to Jacobi sums over a subfield of \mathbb{F}_q .

Lemma 2.11. *Let $p \equiv 3$ or $5 \pmod{8}$, and ψ be a character of order 2^r on \mathbb{F}_q , where*

$$r \geq n = \begin{cases} 3 & \text{if } p \equiv 3 \pmod{8}, \\ 2 & \text{if } p \equiv 5 \pmod{8}, \end{cases}$$

Assume that $2^{r-1} \mid s$. Then $\psi^{2^{r-n}}$ is equal to the lift of some character χ of order 2^n on $\mathbb{F}_{p^{s/2^{r-n+1}}}$. Moreover,

$$G(\psi) = q^{(2^{r-n+1}-1)/2^{r-n+2}} J(\chi) \cdot \begin{cases} 1 & \text{if } p \equiv 3 \pmod{8}, \\ (-1)^{s(r-1)/2^{r-1}} & \text{if } p \equiv 5 \pmod{8}. \end{cases}$$

Proof. We prove the assertion of the lemma by induction on r , for $r \geq n$. Let $2^{n-1} \mid s$ and ψ be a character of order 2^n on \mathbb{F}_q . As $2^n \mid (p^{s/2} - 1)$, Lemma 2.6 shows that ψ is equal to the lift of some character χ of order 2^n on $\mathbb{F}_{p^{s/2}}$, that is, $\chi' = \psi$. Lemmas 2.5 and 2.7 yield $G(\psi) = G(\chi') = -G(\chi)^2 = -G(\chi^2)J(\chi)$. Note that χ^2 has order 2^{n-1} . Thus, by Lemmas 2.3 and 2.4,

$$G(\chi^2) = \begin{cases} -q^{1/4} & \text{if } p \equiv 3 \pmod{8}, \\ (-1)^{(s/2)-1} q^{1/4} & \text{if } p \equiv 5 \pmod{8}, \end{cases}$$

and so

$$G(\psi) = q^{1/4} J(\chi) \cdot \begin{cases} 1 & \text{if } p \equiv 3 \pmod{8}, \\ (-1)^{s/2} & \text{if } p \equiv 5 \pmod{8}. \end{cases}$$

This completes the proof for the case $r = n$.

Suppose now that $r \geq n + 1$, and assume that the result is true when r is replaced by $r - 1$. Let $2^{r-1} \mid s$ and ψ be a character of order 2^r on \mathbb{F}_q . Then $2^{r-2} \mid \frac{s}{2}$, and so $2^r \mid (p^{s/2} - 1)$. By Lemma 2.6, ψ is equal to the lift of some character ϕ of order 2^r on $\mathbb{F}_{p^{s/2}}$, that is $\phi' = \psi$. Applying Lemmas 2.2(c), 2.3, 2.7, 2.8 and using the fact that $2^n \mid s$, we deduce

$$G(\psi) = -G(\phi)^2 = -G(\phi)G(\phi\rho_0) = -\bar{\phi}(4)G(\phi^2)G(\rho_0) = \bar{\phi}(4)q^{1/4}G(\phi^2), \quad (2.1)$$

where ρ_0 denotes the quadratic character on $\mathbb{F}_{p^{s/2}}$. Note that ϕ^2 has order 2^{r-1} and $2^{r-2} \mid \frac{s}{2}$. Hence, by inductive hypothesis, $(\phi^2)^{2^{r-1-n}} = \phi^{2^{r-n}}$ is equal to the lift of some character χ of order 2^n on $\mathbb{F}_{p^{(s/2)/2^{r-n}}} = \mathbb{F}_{p^{s/2^{r-n+1}}}$ and

$$G(\phi^2) = (p^{s/2})^{(2^{r-n}-1)/2^{r-n+1}} J(\chi) \cdot \begin{cases} 1 & \text{if } p \equiv 3 \pmod{8}, \\ (-1)^{(s/2)(r-2)/2^{r-2}} & \text{if } p \equiv 5 \pmod{8}, \end{cases}$$

that is,

$$G(\phi^2) = q^{(2^{r-n}-1)/2^{r-n+2}} J(\chi) \cdot \begin{cases} 1 & \text{if } p \equiv 3 \pmod{8}, \\ (-1)^{s(r-2)/2^{r-1}} & \text{if } p \equiv 5 \pmod{8}. \end{cases}$$

Substituting this expression for $G(\phi^2)$ into (2.1) and using Lemma 2.9, we obtain

$$G(\psi) = q^{(2^{r-n+1}-1)/2^{r-n+2}} J(\chi) \cdot \begin{cases} 1 & \text{if } p \equiv 3 \pmod{8}, \\ (-1)^{s(r-1)/2^{r-1}} & \text{if } p \equiv 5 \pmod{8}. \end{cases}$$

It remains to show that $\psi^{2^{r-n}}$ is equal to the lift of χ . Indeed, for any $x \in \mathbb{F}_q$ we have

$$\begin{aligned} \chi(N_{\mathbb{F}_q/\mathbb{F}_{p^{s/2^{r-n}+1}}}(x)) &= \chi(x^{(p^s-1)/(p^{s/2^{r-n}+1}-1)}) \\ &= \chi((x^{(p^s-1)/(p^{s/2}-1)})^{(p^{s/2}-1)/(p^{s/2^{r-n}+1}-1)}) \\ &= \chi(N_{\mathbb{F}_{p^{s/2}}/\mathbb{F}_{p^{s/2^{r-n}+1}}}(x^{(p^s-1)/(p^{s/2}-1)})) = \phi^{2^{r-n}}(x^{(p^s-1)/(p^{s/2}-1)}) \\ &= \left(\phi(N_{\mathbb{F}_{p^s}/\mathbb{F}_{p^{s/2}}}(x))\right)^{2^{r-n}} = \psi^{2^{r-n}}(x). \end{aligned}$$

Therefore $\chi' = \psi^{2^{r-n}}$, and the result now follows by the principle of mathematical induction. \square

For an arbitrary integer k , it is convenient to set $\eta_k^* = \eta_\ell^*$, where $k \equiv \ell \pmod{e}$, $0 \leq \ell \leq e-1$.

Lemma 2.12. *For any integer k , $\eta_{kp}^* = \eta_k^*$.*

Proof. It is a straightforward consequence of [5, Proposition 1]. \square

From now on we shall assume that $p \equiv 3$ or $5 \pmod{8}$, $e = 2^m$ with $m \geq 3$, and λ is a character of order 2^m on \mathbb{F}_q such that $\lambda(\gamma) = \zeta_{2^m}$. We observe that $2^{m-2} \mid s$.

Lemma 2.13. *We have*

$$P_{2^m}^*(X) = (X - \eta_0^*)(X - \eta_{2^{m-1}}^*) \prod_{t=0}^{m-2} (X - \eta_{2^t}^*)^{2^{m-t-2}} (X - \eta_{-2^t}^*)^{2^{m-t-2}}.$$

Proof. Write

$$\begin{aligned} P_{2^m}^*(X) &= (X - \eta_0^*)(X - \eta_{2^{m-1}}^*) \prod_{t=0}^{m-2} \prod_{\substack{k=1 \\ 2^t \parallel k}}^{2^m-1} (X - \eta_k^*) \\ &= (X - \eta_0^*)(X - \eta_{2^{m-1}}^*) \prod_{t=0}^{m-2} \prod_{\substack{k_0=1 \\ 2 \nmid k_0}}^{2^{m-t}-1} (X - \eta_{2^t k_0}^*). \end{aligned}$$

Since $p \equiv 3$ or $5 \pmod{8}$, $\pm p^0, \pm p^1, \dots, \pm p^{2^{m-t-2}-1}$ is a reduced residue system modulo 2^{m-t} for each $0 \leq t \leq m-2$. Thus

$$P_{2^m}^*(X) = (X - \eta_0^*)(X - \eta_{2^{m-1}}^*) \prod_{t=0}^{m-2} \prod_{j=0}^{2^{m-t-2}-1} (X - \eta_{2^t p^j}^*)(X - \eta_{-2^t p^j}^*).$$

The result now follows from Lemma 2.12. \square

Lemma 2.14. *We have*

$$\begin{aligned}\eta_0^* &= G(\rho) + \sum_{r=2}^m 2^{r-2} \left(G(\lambda^{2^{m-r}}) + G(\bar{\lambda}^{2^{m-r}}) \right), \\ \eta_{2^{m-1}}^* &= G(\rho) + \sum_{r=2}^{m-1} 2^{r-2} \left(G(\lambda^{2^{m-r}}) + G(\bar{\lambda}^{2^{m-r}}) \right) - 2^{m-2} (G(\lambda) + G(\bar{\lambda})),\end{aligned}$$

and, for $0 \leq t \leq m-2$,

$$\begin{aligned}\eta_{\pm 2^t}^* &= \sum_{r=2}^t 2^{r-2} \left(G(\lambda^{2^{m-r}}) + G(\bar{\lambda}^{2^{m-r}}) \right), \\ &+ \begin{cases} -G(\rho) & \text{if } t = 0, \\ G(\rho) - 2^{t-1} \left(G(\lambda^{2^{m-t-1}}) + G(\bar{\lambda}^{2^{m-t-1}}) \right) & \text{if } t > 0, \end{cases} \\ &\mp \begin{cases} 0 & \text{if } p \equiv 3 \pmod{8}, \\ 2^t i \left(G(\lambda^{2^{m-t-2}}) - G(\bar{\lambda}^{2^{m-t-2}}) \right) & \text{if } p \equiv 5 \pmod{8}, \end{cases} \\ &\mp \begin{cases} 2^t i \sqrt{2} \left(G(\lambda^{2^{m-t-3}}) - G(\bar{\lambda}^{2^{m-t-3}}) \right) & \text{if } p \equiv 3 \pmod{8} \text{ and } t \leq m-3, \\ 0 & \text{otherwise.} \end{cases}\end{aligned}$$

Proof. From Lemma 2.1 we deduce that

$$\eta_k^* = \sum_{j=1}^{2^m-1} G(\lambda^j) \zeta_{2^m}^{-jk} = \sum_{r=1}^m \sum_{\substack{j=1 \\ 2^{m-r} \parallel j}}^{2^m-1} G(\lambda^j) \zeta_{2^m}^{-jk} = \sum_{r=1}^m \sum_{\substack{j_0=1 \\ 2 \nmid j_0}}^{2^r-1} G(\lambda^{2^{m-r} j_0}) \zeta_{2^r}^{-j_0 k}.$$

Since $\lambda^{2^{m-r}}$ has order 2^r and, for $r \geq 2$, $\pm p^0, \pm p^1, \dots, \pm p^{2^{r-2}-1}$ is a reduced residue system modulo 2^r , we conclude that

$$\eta_k^* = (-1)^k G(\rho) + \sum_{r=2}^m \sum_{u \in \{\pm 1\}} \sum_{v=0}^{2^{r-2}-1} G(\lambda^{2^{m-r} u p^v}) \zeta_{2^r}^{-k u p^v},$$

or, in view of Lemma 2.2(b),

$$\eta_k^* = (-1)^k G(\rho) + \sum_{r=2}^m \left[G(\lambda^{2^{m-r}}) \sum_{v=0}^{2^{r-2}-1} \zeta_{2^r}^{-k p^v} + G(\bar{\lambda}^{2^{m-r}}) \sum_{v=0}^{2^{r-2}-1} \zeta_{2^r}^{k p^v} \right]. \quad (2.2)$$

The expressions for η_0^* and $\eta_{2^{m-1}}^*$ follow immediately from (2.2). Next we assume that $0 \leq t \leq m-2$. If $r > t+3$, then, by Lemma 2.10,

$$\sum_{v=0}^{2^{r-2}-1} \zeta_{2^r}^{2^t p^v} = \sum_{v=0}^{2^{r-2}-1} \zeta_{2^r}^{-2^t p^v} = 0,$$

and so (2.2) yields

$$\begin{aligned}
\eta_{2^t}^* &= \sum_{r=2}^t 2^{r-2} \left(G(\lambda^{2^{m-r}}) + G(\bar{\lambda}^{2^{m-r}}) \right), \\
&+ \begin{cases} -G(\rho) & \text{if } t = 0, \\ G(\rho) - 2^{t-1} \left(G(\lambda^{2^{m-t-1}}) + G(\bar{\lambda}^{2^{m-t-1}}) \right) & \text{if } t > 0, \end{cases} \\
&+ G(\lambda^{2^{m-t-2}}) \sum_{v=0}^{2^t-1} i^{-p^v} + G(\bar{\lambda}^{2^{m-t-2}}) \sum_{v=0}^{2^t-1} i^{p^v} \\
&+ \begin{cases} G(\lambda^{2^{m-t-3}}) \sum_{v=0}^{2^{t+1}-1} \zeta_8^{-p^v} + G(\bar{\lambda}^{2^{m-t-3}}) \sum_{v=0}^{2^{t+1}-1} \zeta_8^{p^v} & \text{if } t \leq m-3, \\ 0 & \text{if } t = m-2. \end{cases}
\end{aligned}$$

The asserted result now follows from Lemmas 2.4 and 2.10. The expression for $\eta_{-2^t}^*$ can be obtained in a similar manner. \square

3. THE CASE $p \equiv 3 \pmod{8}$

In this section, $p \equiv 3 \pmod{8}$. As before, $2^m \mid (q-1)$ and λ is a character of order 2^m on \mathbb{F}_q with $\lambda(\gamma) = \zeta_{2^m}$.

For $3 \leq r \leq m$, define the integers A_r and B_r by

$$p^{s/2^{r-2}} = A_r^2 + 2B_r^2, \quad A_r \equiv -1 \pmod{4}, \quad p \nmid A_r, \quad (3.1)$$

$$2B_r \equiv A_r(\gamma^{(q-1)/8} + \gamma^{3(q-1)/8}) \pmod{p}. \quad (3.2)$$

It is well known that for each fixed r , the conditions (3.1) and (3.2) determine A_r and B_r uniquely.

Lemma 3.1. *Let r be an integer with $2^{r-1} \mid s$ and $3 \leq r \leq m$. Then*

$$G(\lambda^{2^{m-r}}) + G(\bar{\lambda}^{2^{m-r}}) = 2A_r q^{(2^{r-2}-1)/2^{r-1}}$$

and

$$G(\lambda^{2^{m-r}}) - G(\bar{\lambda}^{2^{m-r}}) = 2B_r q^{(2^{r-2}-1)/2^{r-1}} i\sqrt{2}.$$

Proof. We observe that $\lambda^{2^{m-r}}$ has order 2^r . By Lemma 2.11, $(\lambda^{2^{m-r}})^{2^{r-3}} = \lambda^{2^{m-3}}$ is equal to the lift of some octic character χ on $\mathbb{F}_{p^{s/2^{r-2}}}$ and

$$G(\lambda^{2^{m-r}}) \pm G(\bar{\lambda}^{2^{m-r}}) = q^{(2^{r-2}-1)/2^{r-1}} (J(\chi) \pm J(\bar{\chi})).$$

Note that $\gamma^{(q-1)/(p^{s/2^{r-2}}-1)}$ is a generator of the cyclic group $\mathbb{F}_{p^{s/2^{r-2}}}^*$ and, by the definition of the lift, $\chi(\gamma^{(q-1)/(p^{s/2^{r-2}}-1)}) = \chi(N_{\mathbb{F}_q/\mathbb{F}_{p^{s/2^{r-2}}}}(\gamma)) = \lambda^{2^{m-3}}(\gamma) = \zeta_8$. By [1, Lemma 17], $J(\chi) = A_r + B_r i\sqrt{2}$, and the result follows. \square

We are now in a position to prove the main result of this section.

Theorem 3.2. *Let $p \equiv 3 \pmod{8}$ and $m \geq 4$. Then $P_{2^m}^*(X)$ has a unique decomposition into irreducible polynomials over the rationals as follows:*

(a) if $2^{m-1} \mid s$, then

$$\begin{aligned}
P_{2^m}^*(X) &= (X - q^{\frac{1}{2}} + 4B_3q^{\frac{1}{4}})^{2^{m-2}} (X - q^{\frac{1}{2}} - 4B_3q^{\frac{1}{4}})^{2^{m-2}} \\
&\quad \times (X - q^{\frac{1}{2}} + 8B_4q^{\frac{3}{8}})^{2^{m-3}} (X - q^{\frac{1}{2}} - 8B_4q^{\frac{3}{8}})^{2^{m-3}} \\
&\quad \times \left(X + 3q^{\frac{1}{2}} - \sum_{r=3}^{m-2} 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} + 2^{m-2} A_{m-1} q^{\frac{2^{m-3}-1}{2^{m-2}}} \right)^2 \\
&\quad \times \left(X + 3q^{\frac{1}{2}} - \sum_{r=3}^{m-1} 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} + 2^{m-1} A_m q^{\frac{2^{m-2}-1}{2^{m-1}}} \right) \\
&\quad \times \left(X + 3q^{\frac{1}{2}} - \sum_{r=3}^m 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} \right) \prod_{t=2}^{m-3} Q_t(X)^{2^{m-t-2}};
\end{aligned}$$

(b) if $2^{m-2} \parallel s$ and $m \geq 5$, then

$$\begin{aligned}
P_{2^m}^*(X) &= (X - q^{\frac{1}{2}} + 4B_3q^{\frac{1}{4}})^{2^{m-2}} (X - q^{\frac{1}{2}} - 4B_3q^{\frac{1}{4}})^{2^{m-2}} \\
&\quad \times (X - q^{\frac{1}{2}} + 8B_4q^{\frac{3}{8}})^{2^{m-3}} (X - q^{\frac{1}{2}} - 8B_4q^{\frac{3}{8}})^{2^{m-3}} \\
&\quad \times \left(X + 3q^{\frac{1}{2}} - \sum_{r=3}^{m-2} 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} + 2^{m-2} A_{m-1} q^{\frac{2^{m-3}-1}{2^{m-2}}} \right)^2 \\
&\quad \times \left(\left(X + 3q^{\frac{1}{2}} - \sum_{r=3}^{m-1} 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} \right)^2 + 2^{2(m-1)} A_m^2 q^{\frac{2^{m-2}-1}{2^{m-2}}} \right) \\
&\quad \times \left(\left(X + 3q^{\frac{1}{2}} - \sum_{r=3}^{m-3} 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} + 2^{m-3} A_{m-2} q^{\frac{2^{m-4}-1}{2^{m-3}}} \right)^2 \right. \\
&\quad \left. + 2^{2(m-1)} B_m^2 q^{\frac{2^{m-2}-1}{2^{m-2}}} \right)^2 \prod_{t=2}^{m-4} Q_t(X)^{2^{m-t-2}};
\end{aligned}$$

(c) if $4 \parallel s$, then

$$\begin{aligned}
P_{16}^*(X) &= (X + 3q^{\frac{1}{2}} + 4A_3q^{\frac{1}{4}})^2 (X - q^{\frac{1}{2}} + 4B_3q^{\frac{1}{4}})^4 (X - q^{\frac{1}{2}} - 4B_3q^{\frac{1}{4}})^4 \\
&\quad \times \left((X + 3q^{\frac{1}{2}} - 4A_3q^{\frac{1}{4}})^2 + 64A_4^2 q^{\frac{3}{4}} \right) \left((X - q^{\frac{1}{2}})^2 + 64B_4^2 q^{\frac{3}{4}} \right)^2.
\end{aligned}$$

The integers A_r and $|B_r|$ are uniquely determined by (3.1), and

$$\begin{aligned}
Q_t(X) &= \left(X + 3q^{\frac{1}{2}} - \sum_{r=3}^t 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} + 2^t A_{t+1} q^{\frac{2^{t-1}-1}{2^t}} + 2^{t+2} B_{t+3} q^{\frac{2^{t+1}-1}{2^{t+2}}} \right) \\
&\quad \times \left(X + 3q^{\frac{1}{2}} - \sum_{r=3}^t 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} + 2^t A_{t+1} q^{\frac{2^{t-1}-1}{2^t}} - 2^{t+2} B_{t+3} q^{\frac{2^{t+1}-1}{2^{t+2}}} \right).
\end{aligned}$$

Proof. Since $4 \mid s$, Lemmas 2.3 and 2.4 yield $G(\rho) = G(\lambda^{2^{m-2}}) = G(\bar{\lambda}^{2^{m-2}}) = -q^{1/2}$. Appealing to Lemmas 2.14 and 3.1, we deduce that

$$\eta_0^* = -3q^{\frac{1}{2}} + \sum_{r=3}^{m-1} 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} + 2^{m-2} (G(\lambda) + G(\bar{\lambda})), \quad (3.3)$$

$$\eta_{2^{m-1}}^* = -3q^{\frac{1}{2}} + \sum_{r=3}^{m-1} 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} - 2^{m-2} (G(\lambda) + G(\bar{\lambda})), \quad (3.4)$$

$$\eta_{\pm 2^{m-2}}^* = -3q^{\frac{1}{2}} + \sum_{r=3}^{m-2} 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} - 2^{m-2} A_{m-1} q^{\frac{2^{m-3}-1}{2^{m-2}}}, \quad (3.5)$$

$$\eta_{\pm 2^{m-3}}^* = \begin{cases} q^{\frac{1}{2}} \mp 2i\sqrt{2} (G(\lambda) - G(\bar{\lambda})) & \text{if } m = 4, \\ -3q^{\frac{1}{2}} + \sum_{r=3}^{m-3} 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} \\ -2^{m-3} A_{m-2} q^{\frac{2^{m-4}-1}{2^{m-3}}} \mp 2^{m-3} i\sqrt{2} (G(\lambda) - G(\bar{\lambda})) & \text{if } m \geq 5, \end{cases} \quad (3.6)$$

$$\eta_{\pm 1}^* = q^{\frac{1}{2}} \pm 4B_3 q^{\frac{1}{4}}. \quad (3.7)$$

Moreover, if $m \geq 5$, then

$$\eta_{\pm 2}^* = q^{\frac{1}{2}} \pm 8B_4 q^{\frac{3}{8}} \quad (3.8)$$

and, for $2 \leq t \leq m-4$,

$$\eta_{\pm 2^t}^* = -3q^{\frac{1}{2}} + \sum_{r=3}^t 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} - 2^t A_{t+1} q^{\frac{2^{t-1}-1}{2^t}} \pm 2^{t+2} B_{t+3} q^{\frac{2^{t+1}-1}{2^{t+2}}}. \quad (3.9)$$

Assume that $2^{m-1} \mid s$. Combining (3.3) – (3.9) with Lemma 3.1, we obtain the values of the cyclotomic periods, which are all integers. Part (a) now follows from Lemma 2.13.

Next assume that $2^{m-2} \parallel s$. We have $2^m \parallel (q-1)$, and so $\lambda(-1) = -1$. Hence, by Lemma 2.2(a),

$$(G(\lambda) \pm G(\bar{\lambda}))^2 = G(\lambda)^2 + G(\bar{\lambda})^2 \pm 2\lambda(-1)q = G(\lambda)^2 + G(\bar{\lambda})^2 \mp 2q.$$

Lemmas 2.2(c), 2.3, 2.8, 2.9 and 3.1 yield

$$\begin{aligned} G(\lambda)^2 + G(\bar{\lambda})^2 &= G(\lambda)G(\lambda\rho) + G(\bar{\lambda})G(\bar{\lambda}\rho) = \bar{\lambda}(4)G(\lambda^2)G(\rho) + \lambda(4)G(\bar{\lambda}^2)G(\rho) \\ &= -q^{1/2}(G(\lambda^2) + G(\bar{\lambda}^2)) = -2A_{m-1}q^{(2^{m-2}-1)/2^{m-2}}, \end{aligned}$$

and thus

$$(G(\lambda) \pm G(\bar{\lambda}))^2 = -2q^{(2^{m-2}-1)/2^{m-2}} (A_{m-1} \pm p^{s/2^{m-2}}). \quad (3.10)$$

Note that

$$A_{m-1}^2 + 2B_{m-1}^2 = p^{s/2^{m-3}} = (p^{s/2^{m-2}})^2 = (A_m^2 + 2B_m^2)^2 = (A_m^2 - 2B_m^2)^2 + 2 \cdot (2A_m B_m)^2.$$

Hence $A_{m-1} = \pm(A_m^2 - 2B_m^2)$. Since $p^{s/2^{m-2}} = A_m^2 + 2B_m^2 \equiv 3 \pmod{8}$, B_m is odd, and so $A_{m-1} = A_m^2 - 2B_m^2$. Substituting the expressions for $p^{s/2^{m-2}}$ and A_{m-1} into (3.10),

we find that

$$\begin{aligned} (G(\lambda) + G(\bar{\lambda}))^2 &= -4A_m^2 q^{(2^{m-2}-1)/2^{m-2}}, \\ (G(\lambda) - G(\bar{\lambda}))^2 &= 8B_m^2 q^{(2^{m-2}-1)/2^{m-2}}. \end{aligned}$$

The last two equalities together with (3.3), (3.4) and (3.7) imply

$$\begin{aligned} (X - \eta_0^*)(X - \eta_{2^{m-1}}^*) &= \left(X + 3q^{\frac{1}{2}} - \sum_{r=3}^{m-1} 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} \right)^2 \\ &\quad + 2^{2(m-1)} A_m^2 q^{\frac{2^{m-2}-1}{2^{m-2}}}, \end{aligned} \quad (3.11)$$

$$\begin{aligned} (X - \eta_{2^{m-3}}^*)(X - \eta_{-2^{m-3}}^*) &= \left(X + 3q^{\frac{1}{2}} - \sum_{r=3}^{m-3} 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} + 2^{m-3} A_{m-2} q^{\frac{2^{m-4}-1}{2^{m-3}}} \right)^2 \\ &\quad + 2^{2(m-1)} B_m^2 q^{\frac{2^{m-2}-1}{2^{m-2}}} \quad \text{if } m \geq 5, \end{aligned} \quad (3.12)$$

$$(X - \eta_{2^{m-3}}^*)(X - \eta_{-2^{m-3}}^*) = (X - q^{\frac{1}{2}})^2 + 64B_4^2 q^{\frac{3}{4}} \quad \text{if } m = 4. \quad (3.13)$$

Clearly, the quadratic polynomials on the right sides of (3.11) – (3.13) are irreducible over the rationals.

Putting (3.5), (3.7) – (3.9), (3.11) – (3.13) together and appealing to Lemma 2.13, we deduce parts (b) and (c). This completes the proof. \square

Remark 3.3. The result of Gurak [7, Proposition 3.3(iii)] can be reformulated in terms of A_3 and B_3 . Namely, $P_8^*(X)$ has the following factorization into irreducible polynomials over the rationals:

$$\begin{aligned} P_8^*(X) &= (X - q^{1/2})^2 (X - q^{1/2} + 4B_3 q^{1/4})^2 (X - q^{1/2} - 4B_3 q^{1/4})^2 \\ &\quad \times (X + 3q^{1/2} + 4A_3 q^{1/4}) (X + 3q^{1/2} - 4A_3 q^{1/4}) \quad \text{if } 4 \mid s, \\ P_8^*(X) &= (X - 3q^{1/2})^2 \\ &\quad \times ((X + q^{1/2})^2 + 16A_3^2 q^{1/2}) ((X + q^{1/2})^2 + 16B_3^2 q^{1/2})^2 \quad \text{if } 2 \parallel s. \end{aligned}$$

We see that Theorem 3.2 is not valid for $m = 3$.

4. THE CASE $p \equiv 5 \pmod{8}$

In this section, $p \equiv 5 \pmod{8}$. As in the previous sections, $2^m \mid (q-1)$ and λ denotes a character of order 2^m on \mathbb{F}_q such that $\lambda(\gamma) = \zeta_{2^m}$.

For $2 \leq r \leq m-1$, define the integers C_r and D_r by

$$p^{s/2^{r-1}} = C_r^2 + D_r^2, \quad C_r \equiv 1 \pmod{4}, \quad p \nmid C_r, \quad (4.1)$$

$$D_r \gamma^{(q-1)/4} \equiv C_r \pmod{p}. \quad (4.2)$$

If $2^{m-1} \mid s$, we extend this notation to $r = m$. It is well known that for each fixed r , the conditions (4.1) and (4.2) determine C_r and D_r uniquely.

Lemma 4.1. *Let r be an integer with $2^{r-1} \mid s$ and $2 \leq r \leq m$. Then*

$$G(\lambda^{2^{m-r}}) + G(\bar{\lambda}^{2^{m-r}}) = \begin{cases} -2C_r q^{(2^{r-1}-1)/2^r} & \text{if } 2^r \mid s, \\ (-1)^r \cdot 2C_r q^{(2^{r-1}-1)/2^r} & \text{if } 2^{r-1} \parallel s, \end{cases}$$

and

$$G(\lambda^{2^{m-r}}) - G(\bar{\lambda}^{2^{m-r}}) = \begin{cases} 2D_r q^{(2^{r-1}-1)/2^r} i & \text{if } 2^r \mid s, \\ (-1)^{r-1} \cdot 2D_r q^{(2^{r-1}-1)/2^r} i & \text{if } 2^{r-1} \parallel s. \end{cases}$$

Proof. The proof proceeds exactly as for Lemma 3.1, except that at the end, [8, Proposition 3] is invoked instead of [1, Lemma 17]. \square

We are now ready to establish our second main result.

Theorem 4.2. *Let $p \equiv 5 \pmod{8}$ and $m \geq 4$. Then $P_{2^m}^*(X)$ has a unique decomposition into irreducible polynomials over the rationals as follows:*

(a) *if $2^m \mid s$, then*

$$\begin{aligned} P_{2^m}^*(X) &= (X - q^{\frac{1}{2}} + 2D_2 q^{\frac{1}{4}})^{2^{m-2}} (X - q^{\frac{1}{2}} - 2D_2 q^{\frac{1}{4}})^{2^{m-2}} \\ &\quad \times \left(X + q^{\frac{1}{2}} + \sum_{r=2}^{m-1} 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} - 2^{m-1} C_m q^{\frac{2^{m-1}-1}{2^m}} \right) \\ &\quad \times \left(X + q^{\frac{1}{2}} + \sum_{r=2}^m 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} \right) \prod_{t=1}^{m-2} R_t(X)^{2^{m-t-2}}; \end{aligned}$$

(b) *if $2^{m-1} \parallel s$, then*

$$\begin{aligned} P_{2^m}^*(X) &= (X - q^{\frac{1}{2}} + 2D_2 q^{\frac{1}{4}})^{2^{m-2}} (X - q^{\frac{1}{2}} - 2D_2 q^{\frac{1}{4}})^{2^{m-2}} \\ &\quad \times \left(\left(X + q^{\frac{1}{2}} + \sum_{r=2}^{m-1} 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} \right)^2 - 2^{2(m-1)} C_m^2 q^{\frac{2^{m-1}-1}{2^{m-1}}} \right) \\ &\quad \times \left(\left(X + q^{\frac{1}{2}} + \sum_{r=2}^{m-2} 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} - 2^{m-2} C_{m-1} q^{\frac{2^{m-2}-1}{2^{m-1}}} \right)^2 \right. \\ &\quad \left. - 2^{2(m-1)} D_m^2 q^{\frac{2^{m-1}-1}{2^{m-1}}} \right) \prod_{t=1}^{m-3} R_t(X)^{2^{m-t-2}}; \end{aligned}$$

(c) *if $2^{m-2} \parallel s$, then*

$$\begin{aligned} P_{2^m}^*(X) &= (X - q^{\frac{1}{2}} + 2D_2 q^{\frac{1}{4}})^{2^{m-2}} (X - q^{\frac{1}{2}} - 2D_2 q^{\frac{1}{4}})^{2^{m-2}} \\ &\quad \times \left(\left(X + q^{\frac{1}{2}} + \sum_{r=2}^{m-3} 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} - 2^{m-3} C_{m-2} q^{\frac{2^{m-3}-1}{2^{m-2}}} \right)^2 \right. \\ &\quad \left. - 2^{2(m-2)} D_{m-1}^2 q^{\frac{2^{m-2}-1}{2^{m-2}}} \right)^2 \end{aligned}$$

$$\begin{aligned}
& \times \left(\left(\left(X + q^{\frac{1}{2}} + \sum_{r=2}^{m-2} 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} \right)^2 + 2^{2(m-2)} C_{m-1}^2 q^{\frac{2^{m-2}-1}{2^{m-2}}} + 2^{2m-3} q \right)^2 \right. \\
& \quad \left. - 2^{2(m-1)} C_{m-1}^2 q^{\frac{2^{m-2}-1}{2^{m-2}}} \left(X + (2^{m-2} + 1) q^{\frac{1}{2}} + \sum_{r=2}^{m-2} 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} \right)^2 \right) \\
& \times \prod_{t=1}^{m-4} R_t(X)^{2^{m-t-2}}.
\end{aligned}$$

The integers C_r and $|D_r|$ are uniquely determined by (4.1), and

$$\begin{aligned}
R_t(X) &= \left(X + q^{\frac{1}{2}} + \sum_{r=2}^t 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} - 2^t C_{t+1} q^{\frac{2^t-1}{2^{t+1}}} + 2^{t+1} D_{t+2} q^{\frac{2^{t+1}-1}{2^{t+2}}} \right) \\
&\quad \times \left(X + q^{\frac{1}{2}} + \sum_{r=2}^t 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} - 2^t C_{t+1} q^{\frac{2^t-1}{2^{t+1}}} - 2^{t+1} D_{t+2} q^{\frac{2^{t+1}-1}{2^{t+2}}} \right).
\end{aligned}$$

Proof. As s is even, Lemma 2.3 yields $G(\rho) = -q^{1/2}$. Then, applying Lemmas 2.14 and 4.1, we obtain

$$\begin{aligned}
\eta_0^* &= -q^{\frac{1}{2}} - \sum_{r=2}^{m-2} 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} + 2^{m-3} (G(\lambda^2) + G(\bar{\lambda}^2)) \\
&\quad + 2^{m-2} (G(\lambda) + G(\bar{\lambda})),
\end{aligned} \tag{4.3}$$

$$\begin{aligned}
\eta_{2^{m-1}}^* &= -q^{\frac{1}{2}} - \sum_{r=2}^{m-2} 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} + 2^{m-3} (G(\lambda^2) + G(\bar{\lambda}^2)) \\
&\quad - 2^{m-2} (G(\lambda) + G(\bar{\lambda})),
\end{aligned} \tag{4.4}$$

$$\begin{aligned}
\eta_{\pm 2^{m-2}}^* &= -q^{\frac{1}{2}} - \sum_{r=2}^{m-2} 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} - 2^{m-3} (G(\lambda^2) + G(\bar{\lambda}^2)) \\
&\quad \mp 2^{m-2} i (G(\lambda) - G(\bar{\lambda})),
\end{aligned} \tag{4.5}$$

$$\begin{aligned}
\eta_{\pm 2^{m-3}}^* &= -q^{\frac{1}{2}} - \sum_{r=2}^{m-3} 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} + 2^{m-3} C_{m-2} q^{\frac{2^{m-3}-1}{2^{m-2}}} \\
&\quad \mp 2^{m-3} i (G(\lambda^2) - G(\bar{\lambda}^2)),
\end{aligned} \tag{4.6}$$

$$\eta_{\pm 1}^* = q^{\frac{1}{2}} \pm 2 D_2 q^{\frac{1}{4}}, \tag{4.7}$$

and, for $1 \leq t \leq m-4$,

$$\eta_{\pm 2^t}^* = -q^{\frac{1}{2}} - \sum_{r=2}^t 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} + 2^t C_{t+1} q^{\frac{2^t-1}{2^{t+1}}} \pm 2^{t+1} D_{t+2} q^{\frac{2^{t+1}-1}{2^{t+2}}}. \tag{4.8}$$

First suppose that $2^m \mid s$. By combining (4.3) – (4.8) with Lemma 4.1, we find the values of the cyclotomic periods, which are all integers. Now part (a) follows from Lemma 2.13.

Next suppose that $2^{m-1} \parallel s$. Using (4.3) – (4.8) and Lemma 4.1 again, we find the values of the cyclotomic periods. We observe that η_0^* and $\eta_{2^{m-1}}^*$ as well as $\eta_{2^{m-2}}^*$ and $\eta_{-2^{m-2}}^*$ are algebraic conjugates of degree 2 over the rationals, and the remaining cyclotomic periods are integers. Therefore the polynomials

$$(X - \eta_0^*)(X - \eta_{2^{m-1}}^*) = \left(X + q^{\frac{1}{2}} + \sum_{r=2}^{m-1} 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} \right)^2 - 2^{2(m-1)} C_m^2 q^{\frac{2^{m-1}-1}{2^{m-1}}}$$

and

$$\begin{aligned} (X - \eta_{2^{m-2}}^*)(X - \eta_{-2^{m-2}}^*) &= \left(X + q^{\frac{1}{2}} + \sum_{r=2}^{m-2} 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} - 2^{m-2} C_{m-1} q^{\frac{2^{m-2}-1}{2^{m-1}}} \right)^2 \\ &\quad - 2^{2(m-1)} D_m^2 q^{\frac{2^{m-1}-1}{2^{m-1}}} \end{aligned}$$

are irreducible over the rationals. Part (b) now follows in view of Lemma 2.13.

Finally, suppose that $2^{m-2} \parallel s$. Making use of (4.3) – (4.5) and Lemma 4.1, we obtain

$$\begin{aligned} \eta_0^* &= -q^{\frac{1}{2}} - \sum_{r=2}^{m-2} 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} - (-1)^m \cdot 2^{m-2} C_{m-1} q^{\frac{2^{m-2}-1}{2^{m-1}}} \\ &\quad + 2^{m-2} (G(\lambda) + G(\bar{\lambda})), \end{aligned} \tag{4.9}$$

$$\begin{aligned} \eta_{2^{m-1}}^* &= -q^{\frac{1}{2}} - \sum_{r=2}^{m-2} 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} - (-1)^m \cdot 2^{m-2} C_{m-1} q^{\frac{2^{m-2}-1}{2^{m-1}}} \\ &\quad - 2^{m-2} (G(\lambda) + G(\bar{\lambda})), \end{aligned} \tag{4.10}$$

$$\begin{aligned} \eta_{\pm 2^{m-2}}^* &= -q^{\frac{1}{2}} - \sum_{r=2}^{m-2} 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} + (-1)^m \cdot 2^{m-2} C_{m-1} q^{\frac{2^{m-2}-1}{2^{m-1}}} \\ &\quad \mp 2^{m-2} i (G(\lambda) - G(\bar{\lambda})). \end{aligned} \tag{4.11}$$

By employing the same type of argument as in the proof of Theorem 3.2, we see that

$$(G(\lambda) \pm G(\bar{\lambda}))^2 = \mp 2q^{(2^{m-1}-1)/2^{m-1}} \left(q^{1/2^{m-1}} \pm (-1)^m \cdot C_{m-1} \right).$$

Combining this with (4.9) – (4.11), we conclude that

$$\begin{aligned} (X - \eta_0^*)(X - \eta_{2^{m-1}}^*) &= \left(X + q^{\frac{1}{2}} + \sum_{r=2}^{m-2} 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} + (-1)^m \cdot 2^{m-2} C_{m-1} q^{\frac{2^{m-2}-1}{2^{m-1}}} \right)^2 \\ &\quad + 2^{2m-3} q^{\frac{2^{m-1}-1}{2^{m-1}}} \left(q^{\frac{1}{2^{m-1}}} + (-1)^m \cdot C_{m-1} \right) \end{aligned}$$

and

$$\begin{aligned} & (X - \eta_{2^{m-2}}^*)(X - \eta_{-2^{m-2}}^*) \\ &= \left(X + q^{\frac{1}{2}} + \sum_{r=2}^{m-2} 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} - (-1)^m \cdot 2^{m-2} C_{m-1} q^{\frac{2^{m-2}-1}{2^{m-1}}} \right)^2 \\ & \quad + 2^{2m-3} q^{\frac{2^{m-1}-1}{2^{m-1}}} \left(q^{\frac{1}{2^{m-1}}} - (-1)^m \cdot C_{m-1} \right). \end{aligned}$$

Since $q^{1/2^{m-2}} = p^{s/2^{m-2}} = C_{m-1}^2 + D_{m-1}^2$, we have $q^{1/2^{m-1}} > |C_{m-1}|$. This means that the polynomials $(X - \eta_0^*)(X - \eta_{2^{m-1}}^*)$ and $(X - \eta_{2^{m-2}}^*)(X - \eta_{-2^{m-2}}^*)$ are irreducible over the reals. Furthermore, since $2^{m-2} \parallel s$, the polynomials $(X - \eta_0^*)(X - \eta_{2^{m-1}}^*)$ and $(X - \eta_{2^{m-2}}^*)(X - \eta_{-2^{m-2}}^*)$ belong to $\mathbb{R}[X] \setminus \mathbb{Q}[X]$. Since $\mathbb{R}[X]$ is a unique factorization domain, it follows that the polynomial

$$\begin{aligned} & (X - \eta_0^*)(X - \eta_{2^{m-1}}^*)(X - \eta_{2^{m-2}}^*)(X - \eta_{-2^{m-2}}^*) \\ &= \left(\left(X + q^{\frac{1}{2}} + \sum_{r=2}^{m-2} 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} \right)^2 + 2^{2(m-2)} C_{m-1}^2 q^{\frac{2^{m-2}-1}{2^{m-2}}} + 2^{2m-3} q \right)^2 \\ & \quad - 2^{2(m-1)} C_{m-1}^2 q^{\frac{2^{m-2}-1}{2^{m-2}}} \left(X + (2^{m-2} + 1)q^{\frac{1}{2}} + \sum_{r=2}^{m-2} 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} \right)^2 \end{aligned}$$

is irreducible over the rationals. Further, by Lemma 4.1 and (4.6),

$$\eta_{\pm 2^{m-3}}^* = -q^{\frac{1}{2}} - \sum_{r=2}^{m-3} 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} + 2^{m-3} C_{m-2} q^{\frac{2^{m-3}-1}{2^{m-2}}} \pm (-1)^m \cdot 2^{m-2} D_{m-1} q^{\frac{2^{m-2}-1}{2^{m-1}}},$$

and so $\eta_{2^{m-3}}^*$ and $\eta_{-2^{m-3}}^*$ are algebraic conjugates of degree 2 over the rationals. Hence, the polynomial

$$\begin{aligned} (X - \eta_{2^{m-3}}^*)(X - \eta_{-2^{m-3}}^*) &= \left(X + q^{\frac{1}{2}} + \sum_{r=2}^{m-3} 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} - 2^{m-3} C_{m-2} q^{\frac{2^{m-3}-1}{2^{m-2}}} \right)^2 \\ & \quad - 2^{2(m-2)} D_{m-1}^2 q^{\frac{2^{m-2}-1}{2^{m-2}}} \end{aligned}$$

is irreducible over the rationals. The remaining cyclotomic periods $\eta_{\pm 2^t}^*$, $0 \leq t \leq m-4$, are integers, in view of (4.7) and (4.8). Now Part (c) follows by appealing to Lemma 2.13. This concludes the proof. \square

Remark 4.3. Myerson has shown [10, Theorem 17] that $P_4^*(X)$ is irreducible if $2 \nmid s$,

$$\begin{aligned} P_4^*(X) &= (X + q^{1/2} + 2C_2 q^{1/4})(X + q^{1/2} - 2C_2 q^{1/4}) \\ & \quad \times (X - q^{1/2} + 2D_2 q^{1/4})(X - q^{1/2} - 2D_2 q^{1/4}) \quad \text{if } 4 \mid s, \end{aligned}$$

and, with a slight modification,

$$P_4^*(X) = ((X + q^{1/2})^2 - 4C_2^2 q^{1/2}) ((X - q^{1/2})^2 - 4D_2^2 q^{1/2}) \quad \text{if } 2 \parallel s,$$

where in the latter case the quadratic polynomials are irreducible over the rationals. Furthermore, the result of Gurak [7, Proposition 3.3(ii)] can be reformulated in terms of C_2 ,

D_2 , C_3 and D_3 . Namely, $P_8^*(X)$ has the following factorization into irreducible polynomials over the rationals:

$$\begin{aligned}
P_8^*(X) &= (X - q^{1/2} + 2D_2q^{1/4})^2(X - q^{1/2} - 2D_2q^{1/4})^2 \\
&\quad \times (X + q^{1/2} + 2C_2q^{1/4} + 4C_3q^{3/8})(X + q^{1/2} + 2C_2q^{1/4} - 4C_3q^{3/8}) \\
&\quad \times (X + q^{1/2} - 2C_2q^{1/4} + 4D_3q^{3/8})(X + q^{1/2} - 2C_2q^{1/4} - 4D_3q^{3/8}) \quad \text{if } 8 \mid s, \\
P_8^*(X) &= (X - q^{1/2} + 2D_2q^{1/4})^2(X - q^{1/2} - 2D_2q^{1/4})^2 \\
&\quad \times ((X + q^{1/2} + 2C_2q^{1/4})^2 - 16C_3^2q^{3/4}) \\
&\quad \times ((X + q^{1/2} - 2C_2q^{1/4})^2 - 16D_3^2q^{3/4}) \quad \text{if } 4 \parallel s, \\
P_8^*(X) &= ((X - q^{1/2})^2 - 4D_2^2q^{1/2})^2 \\
&\quad \times \left(((X + q^{1/2})^2 + 4C_2^2q^{1/2} + 8q)^2 - 16C_2^2q^{1/2}(X + 3q^{1/2})^2 \right) \quad \text{if } 2 \parallel s.
\end{aligned}$$

Thus part (a) of Theorem 4.2 remains valid for $m = 2$ and $m = 3$. Moreover, for $m = 3$, part (b) of Theorem 4.2 is still valid (cf. Remark 3.3).

REFERENCES

- [1] I. Baoulina, Generalizations of the Markoff-Hurwitz equations over finite fields, *J. Number Theory* **118** (2006) 31–52.
- [2] I. Baoulina, On the number of solutions to the equation $(x_1 + \cdots + x_n)^2 = ax_1 \cdots x_n$ in a finite field, *Int. J. Number Theory* **4** (2008) 797–817.
- [3] L. D. Baumert and J. Mykkeltveit, Weight distributions of some irreducible cyclic codes, *DSN Progr. Rep.* **16** (1973) 128–131.
- [4] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums* (Wiley-Interscience, New York, 1998).
- [5] S. Gurak, Factors of period polynomials for finite fields, I, in *The Rademacher Legacy to Mathematics*, eds. G. E. Andrews, D. M. Bressoud and L. A. Parson, Contemp. Math., Vol. 166 (American Mathematical Society, 1994), pp. 309–333.
- [6] S. Gurak, Period polynomials for \mathbb{F}_{p^2} of fixed small degree, in *Finite Fields and Applications*, eds. D. Jungnickel and H. Niederreiter (Springer Berlin Heidelberg, 2000), pp. 196–207.
- [7] S. J. Gurak, Period polynomials for \mathbb{F}_q of fixed small degree, in *Number Theory*, eds. H. Kisilevsky and E. Z. Goren, CRM Proc. and Lect. Notes, Vol. 36 (American Mathematical Society, 2004), pp. 127–145.
- [8] S. A. Katre and A. R. Rajwade, Resolution of the sign ambiguity in the determination of the cyclotomic numbers of order 4 and the corresponding Jacobsthal sum, *Math. Scand.* **60** (1987) 52–62.
- [9] R. Lidl and H. Niederreiter, *Finite Fields* (Addison-Wesley, Reading, MA, 1983).
- [10] G. Myerson, Period polynomials and Gauss sums for finite fields, *Acta Arith.* **39** (1981) 251–264.

DEPARTMENT OF MATHEMATICS, MOSCOW STATE PEDAGOGICAL UNIVERSITY, KRASNOPRUD-NAYA STR. 14, MOSCOW 107140, RUSSIA
E-mail address: jbaoulina@mail.ru